identification data is known only to said third party.

2. (Amended) A method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer, to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer; and

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that an identity of said customer is kept from said business entity party,

wherein said business entity is provided with information identifying said customer only as a transactional party in said electronic business transaction, and

wherein said providing an intermediary relationship by said third party comprises replacing an identification data about said first party with an identifier whose linkage to said identification data is known only to said third party.

B1

6. (Amended) The method according to claim 5, wherein said portable device P(C) generates numbers S(C,n), where n is an integer belonging to a set {1, 2, . . . , N}, and

B2

wherein for at least one of a new business entity and another partner of the customer, a new number n is chosen for all further transactions between the customer and said at least one of said new business unit and said another partner.

11. (Amended) The method according to claim 2, wherein, before establishing an intermediary relationship, the customer accesses one or more verifiers Vj, and

B3

wherein the customer identifies itself to each verifier Vj using a number S(C) associated with the proprietary item, and requests Vj to send S(C) to the business entity, together with data verified by Vj.

12. (Amended) The method according to claim 11, wherein communication to the business

entity is performed by appending to the number S(C) a non-identity data relevant to the customer encrypted using pu1(I).

13. (Amended) The method according to claim 11, wherein a link between the third party and the business entity is provided by the third party posting one or more completed application on a dedicated world-wide-web (WWW) page after replacing customer identification data with a number N(T,C, I) which allows the business entity, but no other party, to recognize this number as a number associated with the business entity.

14. (Amended) The method according to claim 2, wherein a payment between a business entity and a third party is documented by a paying party by attaching a tagging number to the payment,

said tagging number being communicated to a bank of the paying party, and accompanies a transaction order to the bank of the payee, and

wherein the paying bank authorizes a money transfer in exchange for a tag coded using a private key of the payee's bank.

B3

B4

16. (Amended) The method according to claim 15, wherein, when a transaction request is submitted, the customer addresses the transaction request to the third party, after selectively consulting with one or more verifiers Vj.

B5

24. (Amended) A method of selecting a purveyor of goods or services in a confidential manner over a network, comprising:

sending, by a customer to a third party, an application and software for encrypting the application using a public key pu1(I),

wherein said application is taken electronically from a business entity,

wherein a public signature scheme of said business entity is (Pr1(I),pu1(I)), software allowing the customer to compute a public signature scheme (Pr2(I,C),pu2(I,C)), and

wherein said business entity is provided with information identifying said customer only as a transactional party in said electronic business transaction, and

wherein said third party replaces an identification data about said customer with an identifier whose linkage to said identification data is known only to said third party.

34. (Amended) A system for conducting business electronically between a first party and a second party, comprising:

means for providing to a third party an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first party and second party; and

means for conducting the electronic business transaction between said first party and second party through the third party such that said identity of said first party is kept from the second party,

wherein said second party is provided with information identifying said first party only as a transactional party in said electronic business transaction, and

wherein said third party replaces an identification data about said first party with an identifier whose linkage to said identification data is known only to said third party.

35. (Amended) A signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for conducting business electronically between a first party and a second party, said method comprising:

providing to a third party an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first and second parties; and

conducting the electronic business transaction between said first and second parties through the third party such that said identity of said first party is kept from the second party,

wherein said second party is provided with information identifying said first party only as a transactional party in said electronic business transaction, and

wherein said third party replaces an identification data about said first party with an identifier whose linkage to said identification data is known only to said third party.

36. (Amended) A system for performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer to a business entity requiring said private data, said system comprising:

means for establishing an intermediary relationship with a third party between the

candidate customer and the business entity;

a proprietary item provided to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer; and

means for performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that an identity of said customer is kept from said business entity party,

wherein said business entity is provided with information identifying said candidate customer only as a transactional party in said electronic commerce, and

wherein said third party replaces an identification data about said customer with an identifier whose linkage to said identification data is known only to said third party.

37. (Amended) A signal-bearing medium tangibly embodying a program of machine- readable instructions executable by a digital processing apparatus to perform a method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer; and

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that an identity of said customer is kept from said business entity,

wherein said business entity is provided with information identifying said customer only as a transactional party in said electronic commerce, and

wherein said third party replaces an identification data about said customer with an identifier whose linkage to said identification data is known only to said third party.

38. (Amended) A method of conducting business electronically between a first party and a second party, comprising:

providing an intermediary relationship with a third party who knows an identity of the

first party but no privacy-compromising information regarding a proposed electronic business transaction between the first party and the second party; and

conducting the electronic business transaction between said first party and said second party through the third party such that said identity of said first party is kept from the second party, but second party can obtain confidential data about first party that do not compromise the identity of said first party,

wherein said third party replaces an identification data about said first party with an identifier whose linkage to said identification data is known only to said third party.

39. (Amended) A method of conducting business electronically between a first party and a second party, comprising:

providing an intermediary relationship with a third party who knows an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first and second parties, said third party enabling communications between the first and second party and having access to the identity but not to the content or the nature of the transaction; and

conducting the electronic business transaction between said first and second parties so that the identity of said first party is not available to the second party,

wherein said second party receives confidential data about said first party unrelated to the identity of said first party, and

wherein said third party replaces an identification data about said first party with an identifier whose linkage to said identification data is known only to said third party.

---

41. (Amended) A method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer, to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing an identity of said customer; and

performing electronic commerce between said customer and said business entity through

said third party, utilizing said proprietary item, such that the identity of said customer is unknown to said business entity,

wherein said third party can recognize, without having access to an identity, each customer to conduct business over an extended period of time and in repeated interactions, and accumulate all data needed to service the customer, to conglomerate such data to provide a customer history or subject the data to data mining technologies, and

wherein said third party replaces an identification data about said customer with an identifier whose linkage to said identification data is known only to said third party.